

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

2 0 0 4 年 7 月 1 6 日

出 願 番 号

Application Number:

特願 2 0 0 4 - 2 0 9 3 6 7

パリ条約による外国への出願  
に用いる優先権の主張の基礎  
となる出願の国コードと出願  
番号

The country code and number  
of your priority application,  
to be used for filing abroad  
under the Paris Convention, is

J P 2 0 0 4 - 2 0 9 3 6 7

出 願 人

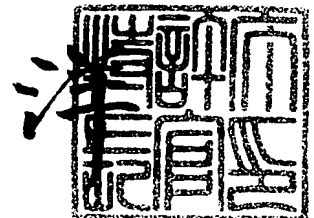
Applicant(s):

日本電信電話株式会社

2 0 0 5 年 5 月 2 0 日

特許庁長官  
Commissioner,  
Japan Patent Office

小 川



【官 規 則】

付 訂 願

【整理番号】

NTTH165462

【提出日】

平成16年 7月16日

【あて先】

特許庁長官 殿

【国際特許分類】

H04L 12/56

【発明者】

【住所又は居所】

東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

【氏名】

松浦 克智

【特許出願人】

【識別番号】

000004226

【氏名又は名称】

日本電信電話株式会社

【代理人】

【識別番号】

100069981

【弁理士】

【氏名又は名称】

吉田 精孝

【電話番号】

03-3508-9866

【手数料の表示】

【予納台帳番号】

008866

【納付金額】

16,000円

【提出物件の目録】

【物件名】

特許請求の範囲 1

【物件名】

明細書 1

【物件名】

図面 1

【物件名】

要約書 1

【包括委任状番号】

9701413

【請求項 1】

グローバルネットワークとプライベートネットワークとの間で、グローバルネットワークからのパケットの宛先アドレスをプライベートアドレスに変換し、プライベートネットワークからのパケットの送信元アドレスをグローバルアドレスに変換することにより、プライベートネットワーク内の複数の端末装置が1つのグローバルアドレスを共有してグローバルネットワーク側の端末装置と通信可能にするアドレス変換装置であって、

プライベートネットワーク内の端末装置に関するグローバルアドレスとプライベートアドレスとの対応関係とともにグローバルネットワーク側のパケット送信元の端末装置のアドレスを送信元アドレスとして含むアドレス変換ルールを記述するアドレス変換テーブルと、

グローバルネットワーク側の端末装置から通信の開始要求を受け付けた時に当該端末装置のアドレスを送信元アドレスとしてプライベートネットワーク内の端末装置に関するグローバルアドレスとプライベートアドレスとの対応関係とともに含むアドレス変換ルールを前記アドレス変換テーブルに追加する機能と、グローバルネットワーク側からパケットを受信した時に宛先アドレスとともに送信元アドレスを含めて前記アドレス変換テーブルを参照して宛先アドレスをプライベートアドレスに変換する機能を有するアドレス変換部とを備えた

ことを特徴とするアドレス変換装置。

【請求項 2】

請求項 1 記載のアドレス変換装置において、

前記アドレス変換部は、前記に加え、

通信終了時に、通信の開始時に追加したアドレス変換ルールをアドレス変換テーブルから削除する機能を有する

ことを特徴とするアドレス変換装置。

【請求項 3】

グローバルネットワークとプライベートネットワークとの間で、グローバルネットワークからのパケットの宛先アドレスをプライベートアドレスに変換し、プライベートネットワークからのパケットの送信元アドレスをグローバルアドレスに変換することにより、プライベートネットワーク内の複数の端末装置が1つのグローバルアドレスを共有してグローバルネットワーク側の端末装置と通信可能にするアドレス変換方法であって、

アドレス変換ルールを記述するアドレス変換テーブルと、アドレス変換部とを少なくとも備えたアドレス変換装置を用い、

アドレス変換部が、

グローバルネットワーク側の端末装置からの通信の開始要求を受け付け時に当該端末装置のアドレスを送信元アドレスとしてプライベートネットワーク内の端末装置に関するグローバルアドレスとプライベートアドレスとの対応関係とともに含むアドレス変換ルールを前記アドレス変換テーブルに追加し、

グローバルネットワーク側からパケットを受信した時に宛先アドレスとともに送信元アドレスを含めて前記アドレス変換テーブルを参照して宛先アドレスをプライベートアドレスに変換する

ことを特徴とするアドレス変換方法。

【請求項 4】

グローバルネットワークとプライベートネットワークとの間で、グローバルネットワークからのパケットの宛先アドレスをプライベートアドレスに変換し、プライベートネットワークからのパケットの送信元アドレスをグローバルアドレスに変換することにより、プライベートネットワーク内の複数の端末装置が1つのグローバルアドレスを共有してグローバルネットワーク側の端末装置と通信可能にするアドレス変換方法であって、

アドレス変換ルールを記述するアドレス変換テーブルと、アドレス変換部とを少なくとも備えたアドレス変換装置を用い、

アドレス変換部が、

グローバルネットワーク側の端末装置からアクセス要求バケットを受け付け、

受け付けたアクセス要求バケット中の送信元アドレスをグローバルネットワーク側のバ

ケット送信元の端末装置のアドレスとして記憶し、

アクセス先の端末装置のプライベートアドレスをアクセス要求元の端末装置に要求し、

アクセス要求元の端末装置からアクセス先の端末装置のプライベートアドレスを受け付け、

プライベートネットワーク内のアクセス先の端末装置に関するグローバルアドレスとプライベートアドレスとの対応関係とともに前記記憶したバケット送信元の端末装置のアドレスを送信元アドレスとして含むアドレス変換ルールをアドレス変換テーブルに追加し、

グローバルネットワーク側からバケットを受信した時に宛先アドレスとともに送信元アドレスを含めて前記アドレス変換テーブルを参照して宛先アドレスをプライベートアドレスに変換する

ことを特徴とするアドレス変換方法。

#### 【請求項 5】

請求項 3 または 4 記載のアドレス変換方法において、

アドレス変換部が、

通信終了時に、通信の開始時に追加したアドレス変換ルールをアドレス変換テーブルから削除する

ことを特徴とするアドレス変換方法。

【発明の名称】 アドレス変換装置及びその方法

【技術分野】

【0001】

本発明は、グローバルネットワークとプライベートネットワークとの間で、グローバルネットワークからのパケットの宛先アドレスをプライベートアドレスに変換し、プライベートネットワークからのパケットの送信元アドレスをグローバルアドレスに変換するアドレス変換技術に関する。

【背景技術】

【0002】

従来より、グローバルネットワークとプライベートネットワークとの間、例えばインターネットとイーサネット（登録商標）等のローカルエリアネットワーク（LAN）との間に配置され、インターネットからLAN内の端末装置へのパケットの宛先アドレスをグローバルIPアドレスからプライベートアドレスに変換し、LAN内の端末装置からインターネットへのパケットの送信元アドレスをプライベートアドレスからグローバルIPアドレスに変換することにより、LAN内のプライベートアドレスしか持たない複数の端末装置が1つのグローバルIPアドレスを共有してインターネットにアクセスできるようにするアドレス変換装置（NAT（Network Address Translation）装置）が知られている。

【0003】

また、インターネット側からのアクセスを、TCP（Transmission Control Protocol）またはUDP（User Datagram Protocol）のポート番号により端末装置に振り分けることにより、インターネットからLAN内の端末装置へのアクセスを可能にするものもある（例えば、特許文献1参照）。

【特許文献1】特開2002-185517号公報

【発明の開示】

【発明が解決しようとする課題】

【0004】

しかしながら、このような従来のアドレス変換装置では、インターネットからLAN内の端末装置へアクセスさせる時にTCPまたはUDPのポート番号を使っているため、1つのポート番号に1つの端末装置しか対応させることができず、同じポート番号で複数の端末装置へアクセスさせることができない、例えばhttp（Hyper Text Transport Protocol）のデフォルトポート番号である80番で複数のサーバを公開できないという問題があった。

【0005】

また、TCPやUDPではないプロトコルで、ポート番号等が無い通信の場合（IPsec（Security Architecture for Internet Protocol）やICMP（Internet Control Message Protocol）等の場合）も、複数の端末装置を公開することができない、例えばIPsecのパケットは1つの端末装置へという設定しかできないため、複数の端末装置で同時にIPsecを使うことができない。これは、LAN内からインターネット側へ向けて通信する場合にも同じように起こるため、LAN内の端末装置でIPsecを利用することは困難である。

【0006】

そこで、本発明は、到達したパケットのソースアドレス（送信元アドレス）も参照してパケットを端末装置に振り分けることにより、同じポート番号で複数のサーバを公開したり、ポート番号の無いプロトコルでも複数の通信を行ったりすることができるアドレス変換装置及びその方法を提供することを目的とする。

【課題を解決するための手段】

【0007】

上記課題を解決する手段として、本発明は、グローバルネットワークとプライベートネットワークとの間で、グローバルネットワークからのパケットの宛先アドレスをプライベ

ードアドレスに変換し、プライベートネットワークからのパケットの送信元アドレスをグローバルアドレスに変換することにより、プライベートネットワーク内の複数の端末装置が1つのグローバルアドレスを共有してグローバルネットワーク側の端末装置と通信可能にするアドレス変換装置であって、プライベートネットワーク内の端末装置に関するグローバルアドレスとプライベートアドレスとの対応関係とともにグローバルネットワーク側のパケット送信元の端末装置のアドレスを送信元アドレスとして含むアドレス変換ルールを記述するアドレス変換テーブルと、グローバルネットワーク側の端末装置から通信の開始要求を受け付けた時に当該端末装置のアドレスを送信元アドレスとしてプライベートネットワーク内の端末装置に関するグローバルアドレスとプライベートアドレスとの対応関係とともに含むアドレス変換ルールを前記アドレス変換テーブルに追加する機能と、グローバルネットワーク側からパケットを受信した時に宛先アドレスとともに送信元アドレスを含めて前記アドレス変換テーブルを参照して宛先アドレスをプライベートアドレスに変換する機能を有するアドレス変換部とを備えたことを特徴とする。

【0008】

これにより、送信元アドレスに対応したアドレス変換ルールが追加され適用される。従って、送信元アドレスが異なっていれば、同じプロトコルやポート番号でも、異なる変換ルールが適用される。

【0009】

また、前記アドレス変換手段は、通信終了時に、通信の開始時に追加したアドレス変換ルールをテーブルから削除する機能を有することが好ましい。

【0010】

これにより、通信終了時には、追加したアドレス変換ルールが削除される。従って、変更した設定による誤ったアクセスを防ぐことができる。

【発明の効果】

【0011】

本発明によれば、グローバルネットワーク側の端末装置からの通信の開始要求により該端末装置のアドレスを送信元とするパケットに対するアドレス変換ルールを追加しているので、送信元アドレスが異なっているパケットには異なった変換ルールを適用させることができ、同じポート番号で複数のサーバを公開したり、ポート番号の無いプロトコルでも複数の通信を行ったりすることができる。

【発明を実施するための最良の形態】

【0012】

以下、図面を参照して本発明を説明する。

【0013】

図1は本発明のアドレス変換装置の実施の形態の一例を示すもので、図中、1はWAN側ネットワークインターフェース部、2はLAN側ネットワークインターフェース部、3はデータベース部、4はアドレス変換部、5は認証処理部である。

【0014】

WAN側ネットワークインターフェース部1は、図示しないインターネット等のワイドエリアネットワーク(WAN)に接続され、WANとのパケットの送受信を行う。LAN側ネットワークインターフェース部2は、図示しないイーサネット等のローカルエリアネットワーク(LAN)に接続され、LANとのパケットの送受信を行う。

【0015】

データベース部3は、アドレス変換テーブルを含むアドレス変換のためのデータ、ユーザ認証のためのデータ等を蓄積している。

【0016】

図2はアドレス変換テーブルの一例を、また、図3は図2のアドレス変換テーブルに後述する如く送信元IPアドレスをソースIPアドレスとして含むアドレス変換ルールが追加された後のアドレス変換テーブルの一例を示すものである。

【0017】

図2、図3において、「ローヘイアドレヘ」の列は、WAN側ネットワークインターフェース部1で受信したパケットの送信元IPアドレスを示している（但し、「any」の場合は任意のアドレスで良い。）。また、「ディスティネーションIPアドレス」の列は、WAN側ネットワークインターフェース部1で受信したパケットの宛先IPアドレスを示している。また、「プロトコル、ディスティネーションポート番号」の列は、WAN側ネットワークインターフェース部1で受信したパケットのプロトコル及び宛先ポート番号を示している。また、「内部IPアドレス」の列は、WAN側ネットワークインターフェース部1で受信したパケットの送信元及び宛先が、当該行のそれぞれの値に一致した時に、そのパケットの宛先IPアドレスに設定するLAN内のプライベートアドレスを示している。また、「プロトコル及びポート番号」の列は、WAN側ネットワークインターフェース部1で受信したパケットの送信元及び宛先が、当該行のそれぞれの値に一致した時に、そのパケットの宛先ポート番号に設定するポート番号を示している。

#### 【0018】

アドレス変換部4は、前述したアドレス変換テーブルに対するアドレス変換ルールの追加・削除を行うとともに、該アドレス変換テーブルに基づいてWAN側ネットワークインターフェース部1及びLAN側ネットワークインターフェース部2で受信したパケットのアドレス変換を行う。

#### 【0019】

即ち、アドレス変換部4は、WAN側ネットワークインターフェース部1で受信したパケットについては、送信元IPアドレス及び宛先IPアドレスにより前記アドレス変換テーブルを参照し、宛先IPアドレスをLAN内のIPアドレス（内部IPアドレス）に変換し、LAN側ネットワークインターフェース部2を介してLAN側に送信する。

#### 【0020】

例えば、図2の1行目では、送信元IPアドレスに関係なく、宛先IPアドレスが「123.123.123.123」でかつ宛先ポート番号が「TCPの443（http:Hyper Text Transfer Protocol Security）」であるパケットは、宛先IPアドレスが「192.168.100.5」に書き替えられ、宛先ポート番号はそのままLAN側に送信される。

#### 【0021】

同様に、図2の2行目では、送信元IPアドレスに関係なく、宛先IPアドレスが「123.123.123.123」でかつ宛先ポート番号が「TCPの22（SSH:Secure Shell）」であるパケットは、宛先IPアドレスが「192.168.100.5」に書き替えられ、宛先ポート番号はそのままLAN側に送信される。

#### 【0022】

また、アドレス変換部4は、LAN側ネットワークインターフェース部2で受信したパケットについては、前記アドレス変換テーブルにおける宛先IPアドレスをグローバルIPアドレスと読み替えた上で、これを内部IPアドレスで参照し、内部IPアドレスをWAN内のグローバルIPアドレスに変換し、WAN側ネットワークインターフェース部1を介してWAN側に送信する。

#### 【0023】

アドレス変換部4では、前述したアドレス変換テーブルを上から受信したパケットの内容により参照し、一致すれば指定された動作を行い、そのパケットに対する処理は終了する。即ち、図2、図3のアドレス変換テーブルでは、上の行に設定された条件がより優先的に処理される条件となっている。

#### 【0024】

認証処理部5は、アドレス変換部4の要求により周知のユーザの認証処理を行う。

#### 【0025】

図4、図5はアドレス変換部における動作の一例を示すフローチャートであり、以下、これに従って本アドレス変換装置の動作を詳細に説明する。

#### 【0026】

アドレス変換部4は、図示しないWAN側の端末装置からWAN側ネットワークインターフェース部1を介して自装置のアドレス宛のhttp（Hyper Text Transfer Protocol）のアクセス要求（通信の開始要求）パケットを受信する（s1）と、アクセス要求パケットの送信元IPアドレスを送信元の端末装置のIPアドレスとして記憶し（s2）、ユーザの認証に必要なユーザの識別情報及びパスワードを入力させるためのHTML（Hyper Text Markup Language）ファイルを、アクセス要求元の端末装置にWAN側ネットワークインターフェース部1を介して送信する（s3）。

#### 【0027】

アドレス変換部4は、アクセス要求元の端末装置からユーザの識別情報及びパスワードを受信する（s4）と、受信したユーザの識別情報及びパスワードを認証処理部5に転送してユーザの認証を要求する（s5）。

#### 【0028】

認証処理部5は、ユーザの識別情報及びパスワードを受信すると、データベース部3に蓄積しているユーザの情報から、受信したユーザ識別情報と一致する識別情報を持つユーザを検索し、一致するユーザが見つければ、蓄積しているそのユーザのパスワードと受信したパスワードを比較し、一致していれば、認証正常をアドレス変換部4に送信する。

#### 【0029】

一致するユーザが見つからなかったり、パスワードが一致しなかった場合は、認証異常をアドレス変換部4に送信する。なお、この際、ユーザに再度、ユーザの識別情報やパスワードの入力を求め、所定の回数繰り返しても一致しない場合に認証異常とするようにしても良い。

#### 【0030】

アドレス変換部4は、認証処理部5から認証正常を受信する（s6）と、アクセスしたいサーバのLAN内部におけるプライベートアドレスやプロトコル、ポート番号等を入力させるためのHTMLファイルをアクセス要求元の端末装置にWAN側ネットワークインターフェース部1を介して送信する（s7）。

#### 【0031】

アクセス要求元の端末装置からプライベートアドレスやプロトコル、ポート番号等を受信する（s8）と、アドレス変換部4は、データベース部3に蓄積しているアドレス変換テーブルに、記憶しているhttpのアクセス要求パケットの送信元IPアドレスをソースIPアドレスとし、受信したプライベートアドレス、プロトコル及びポート番号をそれぞれ内部IPアドレス、プロトコル及びディスティネーションポート番号とした変換ルールを追加する（s9）。

#### 【0032】

例えば、図2のようなテーブルに対して、httpのアクセス要求パケットの送信元IPアドレスが「111.222.234.123」の端末からの、宛先IPアドレス「123.123.123.123」の宛先ポート番号が「TCPの22」のパケットの宛先IPアドレスを、内部IPアドレス「192.168.100.4」に書き替えるようにする場合、図3に示すように、図2のテーブルの一番上の行に、httpによりアクセスしてきた端末のアドレス変換ルールを追加する。

#### 【0033】

これにより、送信元IPアドレスが「111.222.234.123」の宛先ポート番号が「TCPの22」のパケットは、宛先IPアドレスが「192.168.100.4」に書き替えられてLANに送信され、それ以外の送信元IPアドレスの宛先ポート番号が「TCPの22」のパケットは、宛先IPアドレスが「192.168.100.5」に書き替えられてLANに送信されるようになる。

#### 【0034】

その後、アドレス変換部13は、アクセス要求元の端末装置に対して、認証が正常でアドレス変換ルールが設定された旨と、変換先のLAN内部のプライベートアドレスとプロトコルとポート番号等を表示するHTMLファイルを送信する（s10）。

【0035】

アクセス要求元の端末装置では、送信されたHTMLファイルを表示することにより、設定されたアドレス変換の情報を確認することができる。

【0036】

アドレス変換ルールの設定後、アドレス変換部4は、WAN側ネットワークインターフェース部1からパケットを受信する(s12, s14)と、その送信元IPアドレス及び宛先IPアドレスにより前記アドレス変換テーブルを参照し(s15)、宛先IPアドレスをLAN内のIPアドレス(内部IPアドレス)に変換し(s16)、LAN側ネットワークインタフェース部2を介してLANに送信する。

【0037】

また、アドレス変換部4は、LAN側ネットワークインターフェース部2からパケットを受信する(s12, s14)と、その内部IPアドレスにより前記アドレス変換テーブルを参照し(s17)、内部IPアドレスをWAN内のグローバルIPアドレスに変換し(s18)、WAN側ネットワークインターフェース部1を介してWANに送信する。

【0038】

このようにしてLAN内のサーバ(端末装置)との通信を行ったユーザが、通信を終了する場合は、アドレス変換装置から受信したHTMLファイルで表示された画面から通信の終了のボタンを選択して通信終了のパケットを送信するか、当該画面自体を閉じる。

【0039】

アドレス変換装置のアドレス変換部4は、アクセス要求元の端末装置におけるHTML画面の終了に伴う通信の切断を検出する(s11)か、通信終了のパケットを受信する(s13)と、図3のように書き替えたテーブルから追加したルールを削除し(s19)、図2のような元の状態に戻す。

【0040】

このように、本実施の形態においては、httpでアクセスしてきた端末装置の送信元IPアドレスをソースIPアドレスとして、指定されたアドレス変換ルールをアドレス変換テーブルに設定しているので、ソースIPアドレスも含んだ条件によりアドレス変換ルールを設定することができ、同じポート番号でもソースIPアドレスにより別々のサーバへ振り分けたり、ポート番号の無いプロトコルでもソースIPアドレスにより別々の端末と通信を行わせたりすることができる。

【0041】

また、ユーザのリクエストにより、または通信の切断により、変更したアドレス変換ルールの設定を元に戻しているため、変更した設定による誤ったアクセスを防ぐことができる。

【0042】

なお、本実施の形態においては、端末からアドレス変換装置へのアクセスにhttpを使ったが、telnetやSIP(Session Initiation Protocol)等を使ってもかまわない。また、本実施の形態においては、ユーザの認証を行ったが、予め設定された端末からの要求に対しては認証要求を行わないようにしても良い。

【図面の簡単な説明】

【0043】

【図1】 本発明のアドレス変換装置の実施の形態の一例を示すブロック図

【図2】 アドレス変換テーブルの一例を示す図

【図3】 送信元IPアドレスをソースIPアドレスとして含むアドレス変換ルールが追加された後のアドレス変換テーブルの一例を示す図

【図4】 アドレス変換部における動作の一例を示すフローチャート

【図5】 アドレス変換部における動作の一例を示すフローチャート

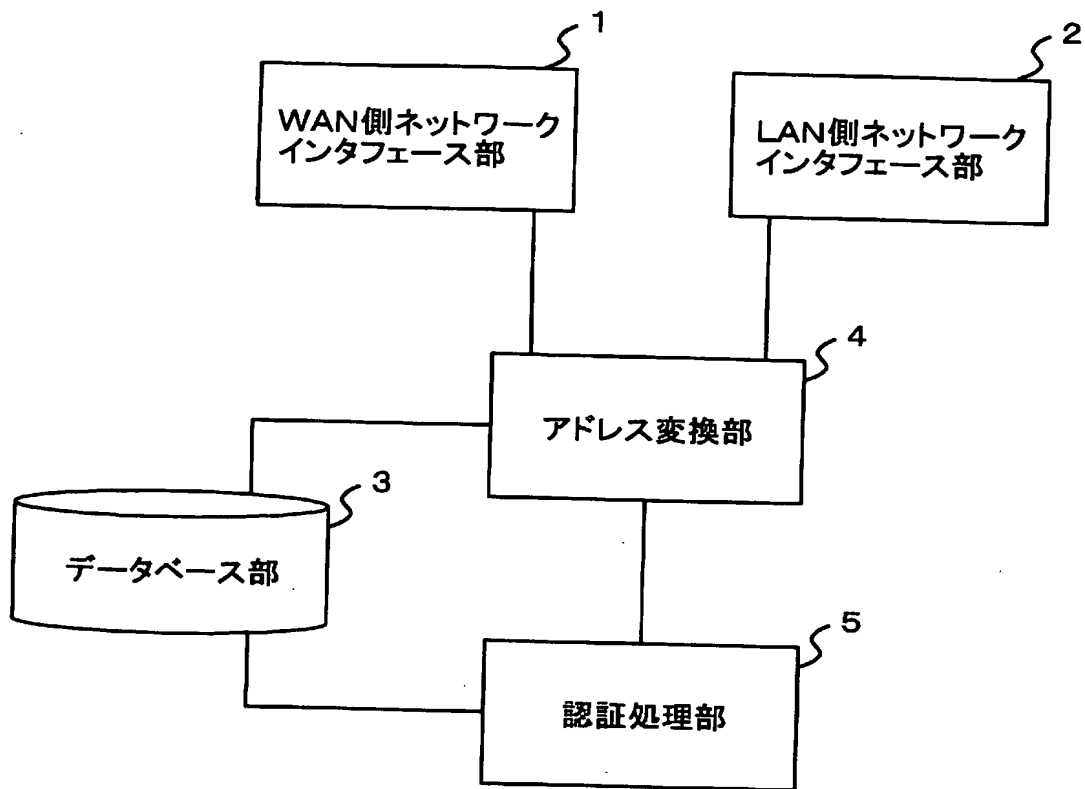
【符号の説明】

【0044】

1：WAN側ネットワークインターフェース部、2：LAN側ネットワークインタフェ

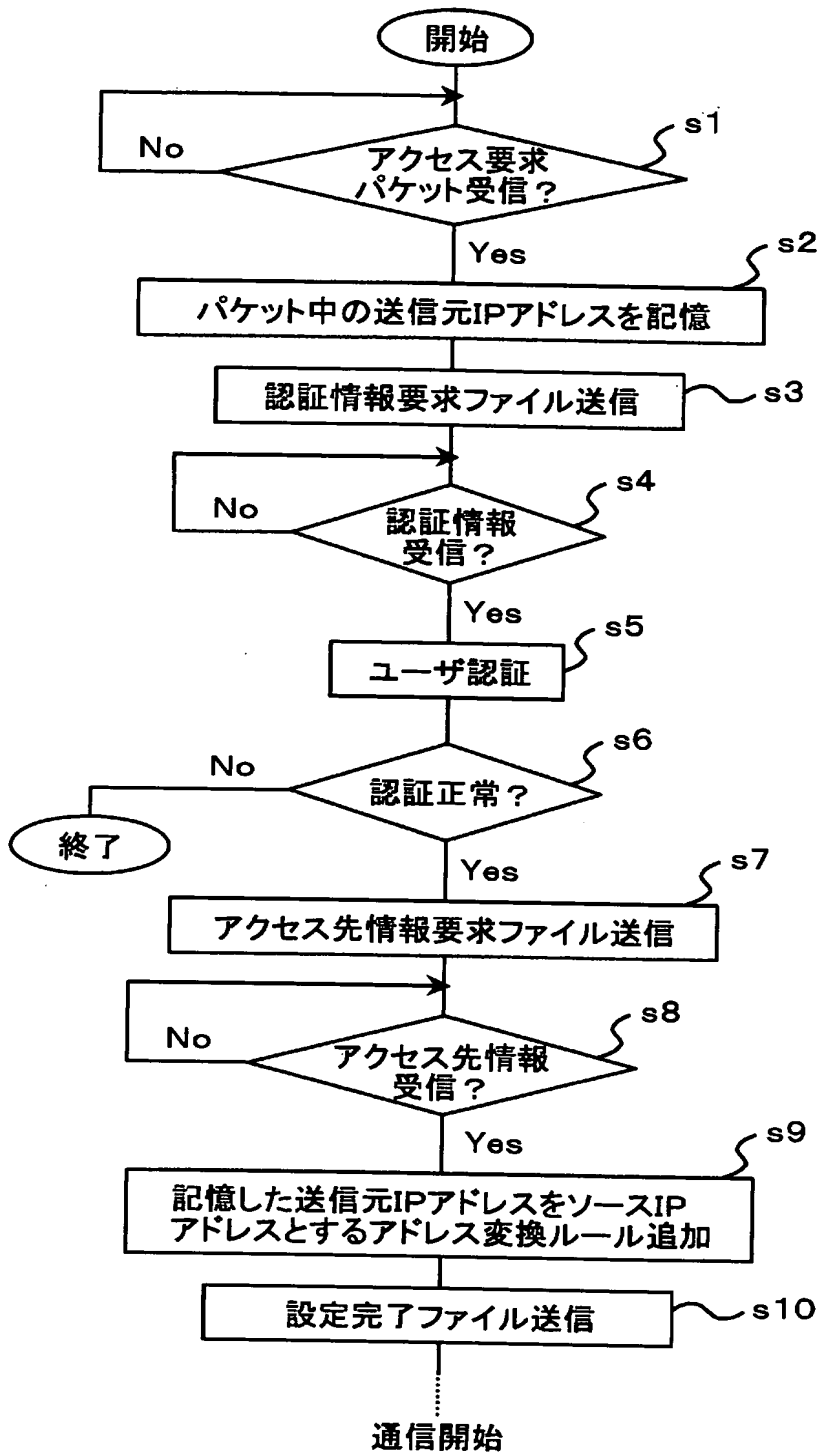
一へ部、ヨ・ノ一ノへ一へ部、サ・ノトレへ交伏部、ヨ・秘祖延埜部。

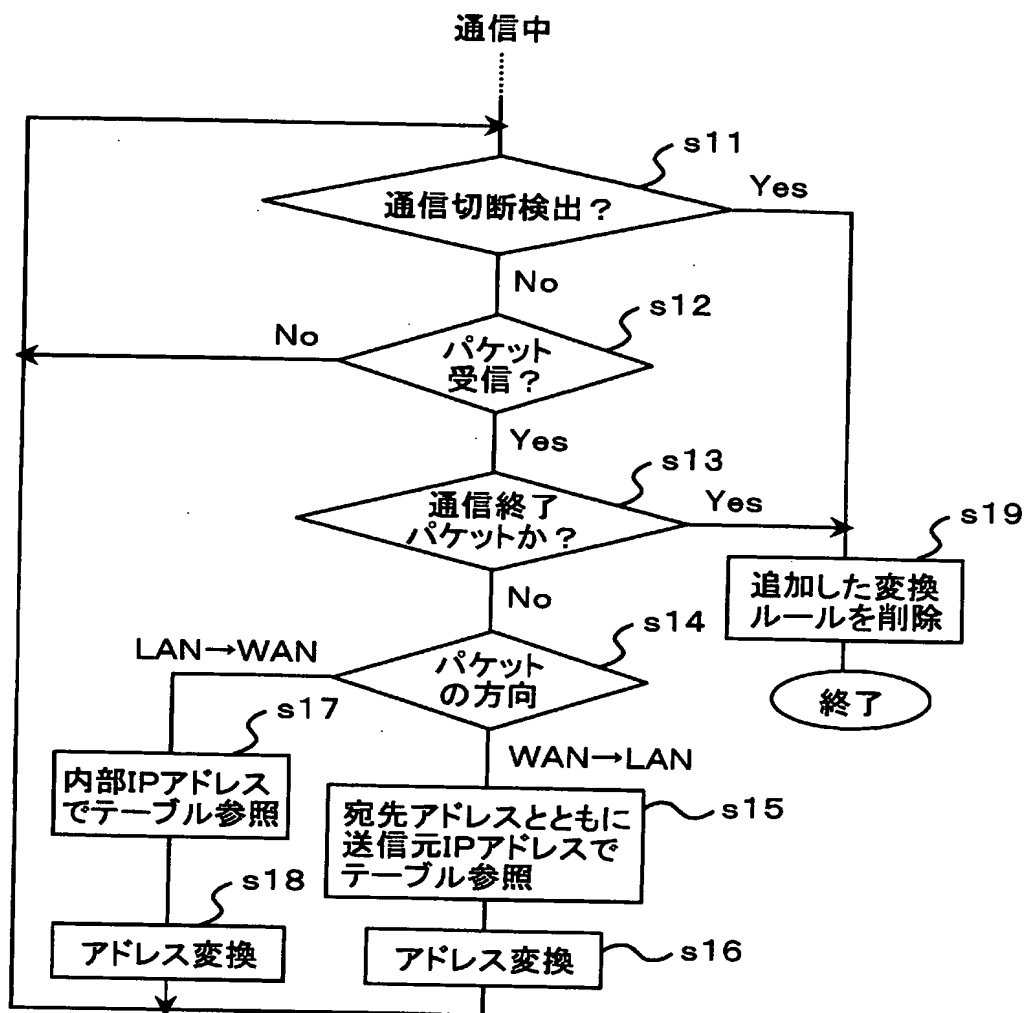
【 図 1 】



ソースIPアドレス	ディスティネーション IPアドレス	プロトコル、 ディスティネーション ポート番号	内部IPアドレス	プロトコル及び ポート番号
any	123.123.123.123	TCP 443	192.168.100.5	TCP 443
any	123.123.123.123	TCP 22	192.168.100.5	TCP 22

ソースIPアドレス	デイスティネーション IPアドレス	プロトコル、 デイスティネーション ポート番号	内部IPアドレス	プロトコル及び ポート番号
111.222.234.123	123.123.123.123	TCP 22	192.168.100.4	TCP 22
any	123.123.123.123	TCP 443	192.168.100.5	TCP 443
any	123.123.123.123	TCP 22	192.168.100.5	TCP 22





【要約】

【課題】 同じポート番号で複数のサーバを公開したり、ポート番号の無いプロトコルでも複数の通信を行ったりすることができるアドレス変換装置を提供すること。

【解決手段】 アドレス変換部4は、WAN側ネットワークインターフェース部1でアクセス要求バケットを受信すると、該バケットの送信元IPアドレスを記憶し、LAN側のアクセス先の端末装置に関する宛先IPアドレスと内部IPアドレスとの対応関係とともに前記記憶した送信元IPアドレスをソースIPアドレスとして含むアドレス変換ルールを、データベース部3に蓄積されたアドレス変換テーブルに追加し、その後、WAN側ネットワークインターフェース部1からバケットを受信すると、送信元IPアドレス及び宛先IPアドレスによりアドレス変換テーブルを参照し、アドレスを変換する。

【選択図】 図1

、

0 0 0 0 0 4 2 2 6

、 19990715

住所変更

5 9 1 0 2 9 2 8 6

東京都千代田区大手町二丁目3番1号

日本電信電話株式会社

# Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/007254

International filing date: 14 April 2005 (14.04.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP  
Number: 2004-209367  
Filing date: 16 July 2004 (16.07.2004)

Date of receipt at the International Bureau: 02 June 2005 (02.06.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland  
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse